THAT WHICH IS CLAIMED IS:

1. A method of performing a Simon's or a Shor's quantum algorithm on a given function ($f(x)$) encoded with a certain number n of qubits, comprising the steps of

carrying out a superposition operation according to one of said quantum algorithms over a set of input vectors, generating a superposition vector (P),

carrying out an entanglement operation (U_F) on said superposition vector (P), generating a corresponding entanglement vector (A),

carrying out an interference operation on said entanglement vector (A), generating a corresponding output vector (B), and

characterized in that

said superposition vector (P) is generated through the following process steps:

calculating, in function of said number n of qubits, the value ($1/2^{n/2}$) of non null components of said superposition vector (P);

calculating indices (i) of the 2^n non null components of said superposition vector as an arithmetical succession, the seed of which is 1 and the common difference of which is 2^n ($i=1+2^n(j-1)$).

2. The method of claim 1, wherein said entanglement vector is generated through the following process steps:

calculating indices (k) of the 2^n non null components of said entanglement vector (A), summing to each term of said arithmetical succession a relative

number corresponding to the value of the given function ($f(j)$) calculated in correspondence of the number of place (j) of said term in said succession ($k = f(j) + 1 + 2^n(j-1)$);

the value of the non null components of said entanglement vector (A) being equal to that of the superposition vector (P).

3. The method of claim 2 for carrying out a Shor's quantum algorithm, comprising the operation of generating real and imaginary components ($\mathrm{Re}[b_h]$, $\mathrm{Im}[b_h]$) of said output vector (B) through the following process steps:

for each index h of said real and imaginary components ($\mathrm{Re}[b_h]$, $\mathrm{Im}[b_h]$), veryfying whether among the terms of the arithmetic succession

$$h \bmod 2^n + 1 + 2^n(j-1)$$

of seed $h \bmod 2^n + 1$, index j and common difference 2^n, there is at least a term corresponding to an index of a non null component of said entanglement vector;

if the above test is negative, making said real and imaginary components ($\mathrm{Re}[b_h]$, $\mathrm{Im}[b_h]$) equal to zero, otherwise calculating said real component ($\mathrm{Re}[b_h]$) as the product between said value of the non null components and the summation of the following cosine functions

$$\cos\left(2\pi \frac{(j-1)\cdot \mathrm{int}[(h-1)/2^n]}{2^n}\right)$$

and said imaginary component ($\mathrm{Im}[b_h]$) as the product between said value of the non null components and the summation of the following sine functions

$$\sin\left(2\pi \frac{(j-1)\cdot \mathrm{int}[(h-1)/2^n]}{2^n}\right)$$

for all values of said index j of said arithmetical succession to which correspond indices (k) of non null components of said entanglement vector.

4. A quantum gate for performing a Simon's or a Shor's quantum algorithm on a given function ($f(x)$) encoded with a certain number n of qubits according to the method of claim 1, comprising

a superposition subsystem carrying out a superposition operation according to one of said quantum algorithms over a set of input vectors, generating a superposition vector (P),

an entanglement subsystem processing said superposition vector (P), generating a corresponding entanglement vector (A),

an interference subsystem processing said entanglement vector (A), generating a corresponding output vector (B), and

characterized in that

said superposition subsystem comprises a circuit generating a first bit string representing said value ($1/2^{n/2}$) of non null components of said superposition vector (P) and other 2^n bit-strings each representing a respective index (i) of the 2^n non null components of said superposition vector;

a memory buffer storing the strings representing said value ($1/2^{n/2}$) and said indices (i).

5. The quantum gate of claim 4, implementing the method of claim 2, wherein said entanglement subsystem comprises

a circuit generating bit-strings representing said indices (k) of the 2^n non null components of said entanglement vector (A);

a second memory buffer storing said bit strings (k).